Security Requirements

**assessment questions**

### 01: Security requirements Basics

Learning Outcome 1.1

1. Security requirements cover both functional security and emergent characteristics
2. True
3. False

Answer: A

Learning Outcome 1.1

1. Which of the following are security goals?
2. Confidentiality
3. Integrity
4. Availability
5. Usability
6. Reliability

Answer: A, B, C

Learning Outcome 1.2

1. Which of the following are true about Authentication and Authorization?
2. Authorization is required before authentication
3. Authentication is required before authorization
4. Authorization is to determine what features a user can access
5. Authentication is to determine who can use the application

Answer: B, C, D

Learning Outcome 1.2

1. Improper authorization requirements can be checked through (select the correct answers)
2. Security auditing
3. Malicious activity detection

Answer: A & B

Learning Outcome 1.2

1. Match the security requirements with description

|  |  |  |
| --- | --- | --- |
| **Security Requirements** | **Selection** | **Description** |
| **Identification, authentication and authorization** | Choose an item. | 1. No parties using the system can deny any of their actions. 2. Ability to examine and review all the actions taken 3. Sensitive data and communication are protected from unauthorized access, both internally and externally. 4. Verify that a user is who he says he is before he can interact with the system. 5. Identify and record all unauthorized access in the system 6. Ensure that all critical data can be recovered in system failure. 7. Unauthorized actions on data, component, and communication are prohibited 8. User can use the service of provided by the application at any time based on a set time requirement. |
| **Integrity** | Choose an item. |
| **Confidentiality** | Choose an item. |
| **Service Availability** | Choose an item. |
| **Non-Repudiation** | Choose an item. |
| **Security Auditing** | Choose an item. |
| **Malicious Activities Detection** | Choose an item. |
| **Backup and Recovery** | Choose an item. |

Answer: D, G, C, H, A, B, E, F

Learning Outcome 1.3

1. Which of the following are true about security requirements?

A. Developing security requirements from the beginning of Software Development Life Cycle (SDLC) will save cost

B. Security requirements should be added after a software system is built

C. Developing security requirements from the beginning of Software Development Life Cycle (SDLC) could reduce business risks

D. Finding security requirements late in the SDLC could increase the time needed to complete the project

Answer: A, C, D

02: Abuse Cases

Learning Outcome 2.1

7) Which of the following are true?

1. Abuse cases are sometimes called misuse cases
2. Abuse cases help developers to think about the software the same way that attackers do
3. Abuse cases help developers to think about negative or unexpected events
4. Abuse cases represent the normative features and functions of the software

Answer: A, B, C

Learning Outcome 2.1

8) Software designers and analysts should carefully consider the implicit assumptions in the system

1. True
2. False

Answer: A

Learning Outcome 2.1

9) Attackers are not likely to undermine the assumptions a system is built on

1. True
2. False

Answer: B

Learning Outcome 2.1

10) One of the goals of abuse case is to decide and document a priori how the software should react to illegitimate use

1. True
2. False

Answer: A

Learning Outcome 2.2

11) Consider a payroll system that allows a human resource department to control salaries and benefits. Which of the following are abuse cases?

1. The system allows users in the HR management group to view and modify salaries of all employees
2. An employee delays payments in order to obtain the extra interest
3. The system will only allow a basic user to view his or her own salary
4. An employee gains extra privileges in the payroll system and slightly increases his own salary

Answer: B, D

Learning Outcome 2.2

12) Consider a client-server application. The architecture had been set up so that the server, which manipulated a financially sensitive database, relied on the client-side application validation, to manage all data-access permissions and no permissions were enforced on the server itself. The client also enforced which messages were sent to the server, the server assumed that any messages coming from the client had passed the client software’s access control system and were, therefore, legitimate. Which of the following are true?

* 1. An attacker may be able to inject data into the database
  2. An attacker may be able to intercept network traffic from client to server
  3. Make the Client Invisible attack pattern is applicable in this situation
  4. An attacker may be able to build a hostile client
  5. An abuse case would be considering what happens when an attacker bypasses the access control mechanism built into the client software

Answer: A, B, C, D, E